

1046 U.S. PTO
10/068677
02/06/02

Express Mail Label Number EL 863955099 US

Attorney's Docket No. 05655.P001

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of:)
David A. Carlson and Vishnu V. Yalala) Art Unit: Not yet assigned
)
Application No: Filed concurrently herewith) Examiner: Not yet assigned
)
Filed: February 6, 2002)
)
For: METHOD AND APPARATUS FOR)
MONTGOMERY MULTIPLICATION)

BOX PATENT APPLICATION

Commissioner for Patents
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT
PURSUANT TO 37 C.F.R § 1.97

Sir:

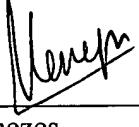
Enclosed is a copy of Information Disclosure Form PTO-1449B together with copies of the cited documents. It is respectfully requested that the cited documents be considered and that the enclosed copy of Information Disclosure Citation Form PTO-1449B be initialed by the Examiner to indicate such consideration, and a copy thereof returned to Applicants.

Pursuant to 37 C.F.R. § 1.97, the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Applicants do not believe any fee is due with this submission, however, should a fee be required, please charge Blakely, Sokoloff, Taylor, & Zafman LLP Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: February 6, 2002


Clive D. Menezes
Reg. No. 45,493

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(512) 330-0844

#44
6-19-02

PTO/SB/08B (10-01)

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Compleat if Known

Application Number	Filed concurrently herewith
Filing Date	February 6, 2002
First Named Inventor	David A. Carlson
Group Art Unit	Not yet assigned
Examiner Name	Not yet assigned
Attorney Docket Number	05655.P001

110466 10/068677 02/06/02

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. 1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T ²
		Blum, T. and Paar, C., "High Radix Montgomery Modular Exponentiation on Reconfigurable Hardware", ECE Department, Worcester Polytechnic Institute, pages 1-13	
		Blum, Thomas, "Modular Exponentiation on Reconfigurable Hardware", Thesis Submitted to the Faculty of Worcester Polytechnic Institute, April 8, 1999, 113 pages	
		Elbirt, AJ and Paar, C., "Towards an FPGA Architecture Optimized for Public-Key Algorithms", Presented at the SPIE's Symposium on Voice, Video, and Comm., 9/20/99, pages 1-10	
		Kim, Chinuk, "VHDL Implementation of Systolic Modular Multiplications on RSA Cryptosystem", Thesis at The City College of the City University of New York, Jan. 2001, 43 pages	
		Gutub, Adnan, "A Modulo Multiplication Hardware Design", Project Report at Oregon State University, Electrical & Computer Engineering Department, Winter 2000, 8 pages	
		Poldre, J. et al., "Modular Exponent realization on FPGAs", Tallinn Technical University, Computer Engineering Department, 12 pages	
		Savas, E. et al., "A Scalable and Unified Multiplier Architecture for Finite Fields GF(p) and GF(2 ^m)", Oregon State University, Electrical and Computer Engineering, 20 pages	
		Shand, M. et al., "Fast Implementation of RSA Cryptography", Digital Equipment Corp., Paris Research Laboratory, 9 pages	
		Tanca, Alexandre F. and Koc, Cetin K., "A Scalable Architecture For Montgomery Multiplication", Oregon State University, Electrical and Computer Engineering Department, 13 pages	
		"How SSL Works", http://developer.netscape.com/tech/security/ssl/howitworks.html , 6/1/01	
		Savolainen, Sampo, "Internet Key Exchange (IKE)", Helsinki University of Technology, Department of Electrical and Communications Engineering, November 22, 1999, http://www.niksula.cs.hut.fi/sjsavola/SoN/essay.html , 12 pages	

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO				<i>Complete if Known</i>	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				Application Number	Filed concurrently herewith
				Filing Date	February 6, 2002
				First Named Inventor	David A. Carlson
				Group Art Unit	Not yet assigned
				Examiner Name	Not yet assigned
Sheet	2	of	2	Attorney Docket Number	05655.P001

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

***EXAMINER:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). **2** Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.